

Министерство образования и науки Российской Федерации
ФГБОУ ВО «Уральский государственный педагогический университет»
Институт математики, информатики и информационных технологий
Кафедра высшей математики

Применение прикладного пакета GАР к типовой классификации четырехмерных алгебр

Выпускная квалификационная работа

Квалификационная работа
допущена к защите
Зав. кафедрой

дата подпись

Исполнитель:
Яговитина Юлия Сергеевна,
студентка группы БП-41

подпись

Руководитель ОПОП:

подпись

Научный руководитель:
Коробков С.С.,
к.ф.-м.н., доцент

подпись

Екатеринбург 2016

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
ГЛАВА I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ	6
1.1. Понятие алгебры над полем. Примеры алгебр	6
1.2. Понятие подалгебры. Признак подалгебры	7
1.3. Алгебраические элементы колец.....	7
1.4. Понятие решетки. Основные свойства решеток	8
1.5. Диаграммы решеток.....	10
1.6. Решетка подалгебр алгебры над полем	12
1.7. Пировские разложения колец.....	12
ГЛАВА II. СИСТЕМА КОМПЬЮТЕРНОЙ АЛГЕБРЫ GAP	14
2.1. Общая характеристика пакета GAP	14
2.2. Общие команды пакета	16
2.3. Команды для вычислений в алгебрах.....	17
ГЛАВА III. ТИПОВАЯ КЛАССИФИКАЦИЯ ПОДАЛГЕБР ЧЕТЫРЕХМЕРНОЙ АЛГЕБРЫ МАТРИЦ $M(GF(2),3)$	21
3.1. Подалгебры четырехмерной алгебры матриц над полем из двух элементов	21
3.2. Вычисление типа подалгебры.	23
3.3. Определение отношения покрытия	25
3.4. Построение диаграммы решетки.....	29
3.5. Типы решеток подалгебр четырехмерных подалгебр	41
3.6. Классификация четырехмерных подалгебр в алгебре матриц третьего порядка над полем из двух элементов	42
БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	45
ПРИЛОЖЕНИЯ	46

ВВЕДЕНИЕ

Актуальность темы исследований. При изучении решеток подалгебр ассоциативных алгебр довольно часто приходится прибегать к примерам для того, чтобы проверить те или иные предположения. Для построения примера может потребоваться много времени, а иногда одного примера бывает недостаточно. Удобно, когда имеется большой набор самых разных примеров, к которым можно обратиться и быстро решить возникший вопрос.

Выпускная квалификационная работа посвящена алгебре $A = M(GF(2), 3)$ матриц порядка 3 над полем из двух элементов. Из результатов, полученных ранее [11], известно, что алгебра A содержит ровно 2100 собственных подалгебр. Порядки этих подалгебр являются степенями числа 2: $2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7$. Хотя сама алгебра A имеет порядок 2^9 , но она не содержит подалгебр порядка 2^8 . Основными объектами исследования являются некоторые четырехмерные подалгебры алгебры A . В работе используется понятие типа решетки подалгебр. Приведем его.

Пусть S – подалгебра алгебры A . Упорядоченную последовательность неотрицательных целых чисел

$$(a_0, a_1, \dots, a_n), \quad (1)$$

назовем типом решетки подалгебр алгебры S , если a_i – количество подалгебр порядка 2^i в алгебре S . Отметим несколько простых свойств типов подалгебр. Прежде всего, заметим, что $a_0 = a_n = 1$, так как a_0 – число подалгебр порядка 1 (нулевая подалгебра единственна), a_n – количество подалгебр максимального порядка в подалгебре S (то есть сама подалгебра S). Длина последовательности (1) равна числу $(n+1)$, а число n определяется из равенства $2^n = |S|$. Заметим, что некоторые из чисел a_1, \dots, a_{n-1} могут равняться нулю, например, если $(1, 1, 0, 1)$ – тип некоторой подалгебры S , то это означает, что S содержит по одной подалгебре порядков $2^0, 2^1, 2^3$ и не содержит подалгебр порядка 2^2 .

Основная цель выпускной квалификационной работы состоит в описании решеток подалгебр четырехмерных алгебр, содержащихся в алгебре A . Для достижения этой цели решаются следующие задачи:

- 1) построение множества порождающих элементов алгебры A ;
- 2) нахождение подалгебр порядка 16;
- 3) вычисление для каждой из отобранных подалгебр типа решетки подалгебр;
- 4) классификация подалгебр по типам;
- 5) решение вопроса об изоморфизме решеток для каждого найденного типа.

Для каждого найденного типа решетки осуществляется классификация с точностью до изоморфизма алгебр. При этом сами подалгебры описываются на языке порождающих элементов и определяющих соотношений.

Данная работа содержит введение, три главы, библиографический список, а так же приложения, на которые имеются ссылки в тексте работы. Первая глава носит теоретический характер. В ней рассматриваются различные алгебраические элементы (идемпотентные и нильпотентные элементы) и их свойства.

Во второй главе подробно описана система компьютерной алгебры GAP. Здесь представлены характеристики данного пакета, указывается какие задачи можно решать с помощью пакета GAP.

В третьей главе исследуется вопрос об изоморфизме решеток подалгебр, имеющих один и тот же тип. Приведем основные результаты этой главы:

Теорема 1. В алгебре A существует всего 21 подалгебра с решеткой типа $(1, 6, 8, 4, 1)$. Все эти подалгебры изоморфны между собой, а значит, имеют изоморфные решетки подалгебр.

Теорема 2. В алгебре A существует всего 84 подалгебры с решеткой типа $(1, 9, 13, 4, 1)$. Все эти подалгебры разбиваются на 4 подмножества,

содержащие по 21 подалгебре. В каждом классе все подалгебры изоморфны между собой, а подалгебры их различных классов – не изоморфны.

Теорема 3. В алгебре A существует всего 42 подалгебры с решеткой типа $(1, 9, 11, 5, 1)$. Все эти подалгебры разбиваются на 2 подмножества, содержащие по 21 подалгебре. В каждом классе все подалгебры изоморфны между собой, а подалгебры их различных классов – не изоморфны.

ГЛАВА I. Теоретические основы

1.1. Понятие алгебры над полем. Примеры алгебр

Определение 1. Алгеброй над полем P называется множество A , на котором определены две бинарные операции $+$ и \cdot , а также операция умножения элементов из P на элементы из A (то есть отображение $P \times A \rightarrow A$), удовлетворяющие следующим условиям:

1. $(A, +, \cdot)$ - кольцо
2. $(A, +)$ - векторное пространство над полем P
3. $\forall \alpha \in P \forall a, b \in A (\alpha a)b = \alpha(ab) = a(\alpha b)$.

Определение 2. Пусть A – алгебра над полем P . Назовем алгебру A конечномерной, если A , как векторное пространство над полем P , конечномерно. При этом, размерность векторного пространства A над P будем называть размерностью или рангом алгебры A .

Пример 1.

Пусть $M_n(F) = \{(\alpha_{ij} \mid \alpha_{ij} \in F)\}$ - множество всех квадратных матриц с коэффициентами из поля F . Ясно, что $M_n(F)$ – кольцо относительно операций сложения и умножения квадратных матриц. Если определить умножение элементов из F на элементы из $M_n(F)$ следующим образом: $\forall \beta \forall (\alpha_{ij}) \in M_n(F) \beta(\alpha_{ij}) = (\beta \alpha_{ij})$, то относительно такого умножения и сложения матриц множество $M_n(F)$ становится векторным пространством над полем F . Следовательно, $M_n(F)$ – алгебра над полем F . Эта алгебра называется алгеброй матриц над полем F .

Пример 2.

Пусть V – n -мерное пространство над полем F и $\Phi_n(F)$ – множество всех линейных преобразований пространства V . Известно, что $\Phi(F)$ – алгебра над полем F относительно следующих операций:

1. $\forall \varphi, \psi \Phi_n(F) \forall v \in V (\varphi + \psi)(v) = \varphi(v) + \psi(v);$
2. $\forall \varphi, \psi \Phi_n(F) \forall v \in V (\varphi \circ \psi)(v) = \psi(\varphi(v));$
3. $\forall \varphi, \psi \Phi_n(F) \forall \alpha \in F (\alpha \varphi(a) = \alpha(\varphi(a))).$

1.2. Понятие подалгебры. Признак подалгебры

Определение 3. Подмножество S алгебры A над полем F назовем подалгеброй алгебры, если относительно операций, определенных в A , S – само является алгеброй над полем F .

Теорема. (признак подалгебры). Непустое подмножество S алгебры A над полем F тогда и только тогда является подалгеброй в A , когда выполнены следующие условия:

1. $\forall a, b \in S (a - b) \in S;$
2. $\forall a, b \in S (ab) \in S;$
3. $\forall \alpha \in P \forall a \in S \alpha a \in S.$

Доказательство: пусть S – подалгебра алгебры A . Тогда очевидно, что условия 1-3 выполнены. Обратно: пусть выполнены условия 1-3. Тогда из выполнимости условий 1 и 2 следует, что S – подкольцо кольца, а из выполнимости условий 1-3 следует, что S – векторное подпространство пространства A . Условие 3 выполняется в S , так как оно выполняется в A . Таким образом, S – подалгебра алгебры A .

1.3. Алгебраические элементы колец

Любая алгебра является кольцом с операциями сложения $(+)$ и умножения (\cdot) $A = (A, +, \cdot, \times), P$ – поле, $P = GF(2) = \{0, 1\}$.

Определение 4. Элемент e кольца K называется *идемпотентным* элементом, если выполняется условие: $e^2 = e$.

Пример 3. 1 – в кольце Z .

$$m = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} m^2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Определение 5. Элемент r кольца K называется *нильпотентным*, если $\exists n \in \mathbb{N}: r^n = 0$. Наименьший n с таким свойством называется *индексом* *нильпотентности* элемента n ($\text{indr} = n$).

Пример 4.

$$\begin{aligned} 0^2 &= 0, \text{indr} = 1 \\ r &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} r^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0, \\ \text{indr} &= 2 \\ m &= \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} m^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} m^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \\ \text{ind} m &= 3 \end{aligned}$$

Определение 6. Элемент a кольца K называется *алгебраическим*, если существует многочлен положительной степени $f(x)$ с целым коэффициентом, то есть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x$ такой, что $f(a) = 0$.

1.4. Понятие решетки. Основные свойства решеток

Введем основные понятия для решетки:

Решеткой называется частично упорядоченное множество, в котором каждое двухэлементное подмножество имеет нижнюю и верхнюю грани.

Полной решеткой называется частично упорядоченное множество, в котором каждое подмножество имеет нижнюю и верхнюю грани.

Верхней гранью подмножества S частично упорядоченного множества называется наименьший элемент в множестве верхних границ подмножества S .

Верхней границей подмножества S частично упорядоченного множества (P, \geq) называется элемент $a \in P$, удовлетворяющий условию $(\forall s \in S s \leq a)$.

Верхнюю грань подмножества S в подмножестве $T \subseteq P$ обозначают выражением $\sup_T S$. При этом, если $T=P$, то индекс T опускают.

Двойственными понятиям верхней границы и верхней грани являются понятия *нижней границы* и *нижней грани*. Нижнюю грань называют также

инфимумом. Другими словами, инфимум – это наибольшая из всех нижних граней. Нижнюю грань подмножества S в подмножестве $T \subseteq P$ обозначают символом $\inf_T S$.

Свойства решеток \mathbf{x} .

В любой решетке (L, \wedge, \vee) операции объединения и пересечения удовлетворяют условию *изотонности*: если $x \leq y$, то $x \wedge z \leq z \wedge y$ и $x \vee z \leq z \vee y$.

Доказательство: Согласно определению 3 из свойств решетки, следует, что если $x \leq y$, то, $x \wedge z = (y \wedge x) \wedge (z \wedge z) = (x \wedge z) \wedge (z \wedge y)$ откуда $x \wedge z \leq z \wedge y$ вследствие совместимости. Второе неравенство $x \vee z \leq z \vee y$ доказывается двойственно (принцип двойственности).

Во всякой решетке (L, \wedge, \vee) выполняются следующие неравенства дистрибутивности: $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$; $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$.

Доказательство:

По свойству совместимости $x \wedge y \leq x$ и $x \wedge y \leq y \leq y \vee z$, откуда следует, что $x \wedge y \leq x \wedge (y \vee z)$. Также $x \wedge z \leq x$ и $x \wedge z \leq z \leq y \vee z$, откуда следует, что $x \wedge z \leq x \wedge (y \vee z)$. Таким образом, $x \wedge (y \vee z)$ является верхней гранью для $x \wedge y$ и $x \wedge z$, и значит, выполняется неравенство $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.

По свойству совместимости $x \leq x \vee y$ и $y \wedge z \leq y \leq x \vee y$ откуда следует, что $x \vee (y \wedge z) \leq x \vee y$, также $x \leq x \vee z$ и $y \wedge z \leq z \leq x \vee z$ откуда следует, что $x \vee (y \wedge z) \leq x \vee z$. Таким образом, $x \vee (y \wedge z)$ является нижней гранью для $x \vee y$ и $x \vee z$, и значит, выполняется неравенство $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$.

Во всякой решетке (L, \wedge, \vee) выполняется неравенство модулярности: если $x \leq z$, то $x \vee (y \wedge z) \leq (x \vee y) \wedge z$.

Доказательство: $x \leq x \vee y$ и $x \leq z$, значит, $x \leq (x \vee y) \wedge z$. Аналогично, $y \wedge z \leq y \leq x \vee y$ и $y \wedge z \leq z$.

Следовательно, $y \wedge z \leq (x \vee y) \wedge z$, откуда $x \vee (y \wedge z) \leq (x \vee y) \wedge z$.

1.5. Диаграммы решеток

Назовем элементы a и b частично упорядоченного множества (P, \leq) сравнимыми, если $a \leq b$ или $b \leq a$. Будем говорить, что элемент b покрывает элемент a , если выполнены следующие условия:

1) $a < b$;

2) $\forall c \in P ((a \leq c) \wedge (c \leq b) \Rightarrow (c = a) \vee (c = b))$.

Если b покрывает a , то будем записывать это кратко так: $a < b$.

В ряде случаев ч.у. множество может быть наглядно изображено в виде диаграммы на плоскости. Для того чтобы изобразить ч.у. множество (P, \leq) в виде диаграммы, примем следующие соглашения:

1) различные элементы множества P изображаются различными точками плоскости;

2) если $a, b \in P$ и b покрывает a , то точки, изображающие эти элементы, соединяются отрезком, причем точка, соответствующая b , располагается выше точки, соответствующей a .

Понятно, что диаграмма может быть построена полностью лишь в том случае, когда ч.у. множество P конечно. Однако при этом она может быть достаточно сложной и потому бесполезной. Очевидно также и то, что при построении диаграммы ее отрезки могут пересекаться в точках, не изображающих элементы множества P . Диаграмма, содержащая минимальное число таких пересечений, называется оптимальной, а не содержащая их совсем - плоской.

Рассмотрим примеры ч.у. множеств и их диаграмм.

Пример а. $P = (M, \leq)$, где $M = \{1, 2, 5, 7\}$;

Пример б. $S = (M, |)$, где $M = \{1, 2, 3, 6, 10\}$;

Пример в. $T = (M, |)$, где $M = \{2, 3, 4, 6, 12\}$;

Пример г. $V = (M, |)$, где $M = \{2, 3, 5, 7\}$.

Диаграммы этих множеств представлены на рис. 1

а) – г) соответственно.

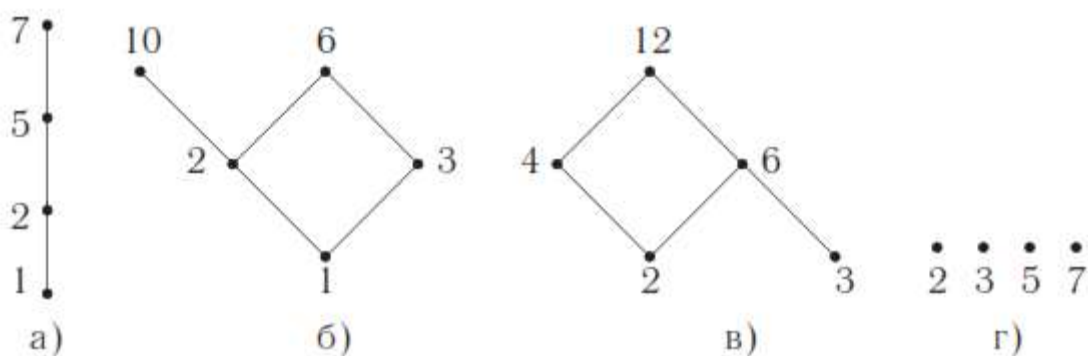


Рис.1

Рассмотрим еще три примера.

Пример 5. $U = (V(M), \subseteq)$, где $M = \{1, 2, 3\}$;

Пример 6. (M, ρ) , где $M = \{a, b, c, d, e\}$, $\rho = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (a, e), (b, e), (c, e), (d, e)\}$;

Пример 7. (M, ρ) , где $M = \{a, b, c, d, e\}$,
 $\rho = (a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (a, e), (b, c), (b, e), (c, e), (d, e)\}$.

Диаграммы этих множеств представлены на рис. 2 а) – в) соответственно.

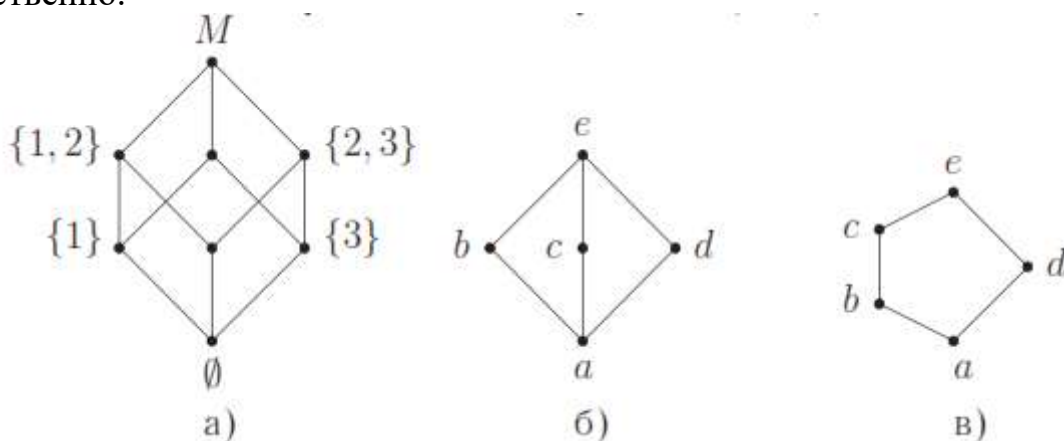


Рис.2

Решение вопроса о том, является ли конечное ч.у. множество P решеткой, может быть значительно сокращено, если имеется диаграмма этого множества. В этом случае для того, чтобы найти верхнюю грань двухэлементного подмножества $\{a, b\}$ нужно, во-первых, найти расположенные выше a и b общие точки, соединенные с ними, и, во-вторых, выбрать среди таких точек ту,

которая была бы расположена ниже всех и соединена со всеми ними. Двойственным образом находится нижняя грань подмножества $\{a, b\}$

1.6. Решетка подалгебр алгебры над полем

Теорема 2: Пусть $L(A)$ – алгебра над полем P . Тогда $(L(A), \wedge, \vee)$ – решетка.

Доказательство. Проверим выполнимость четырех аксиом решетки для $(L(A), \wedge, \vee)$.

1) Идемпотентность. $\forall B \in L(A) \quad B \wedge B = B \cap B = B;$

$$B \vee B = \langle B \cup B \rangle = \langle B \rangle = B.$$

2) Коммутативность. $\forall B, C \in L(A) \quad B \wedge C = B \cap C = C \cap B = C \wedge B; \quad B \vee C = \langle B \cup C \rangle = \langle C \cup B \rangle = C \vee B.$

3) Ассоциативность. $\forall B, C, D \in L(A), \quad B \wedge (C \wedge D) = B \cap (C \cap D) = (B \cap C) \cap D = (B \wedge C) \wedge D$ и $B \vee (C \vee D) = B \vee \langle C \cup D \rangle = \langle B \cup \langle C \cup D \rangle \rangle = \langle B \cup (C \cup D) \rangle = \langle (B \cup C) \cup D \rangle = \langle \langle B \cup C \rangle \cup D \rangle = \langle B \cup C \rangle \vee D = (B \vee C) \vee D.$

4) Поглощение. $\forall B, C \in L(A) \quad B \wedge (B \vee C) = B \cap \langle B \cup C \rangle = B$ и $B \vee (B \wedge C) = B \vee (B \cap C) = B.$

1.7. Пировские разложения колец

Пусть K – коммутативное кольцо, e – ненулевой идемпотентный элемент.

Определим два множества:

$$eK = \{ex | x \in K\} \neq \emptyset$$

$$(1 - e)K = \{x - ex | x \in K\} \neq \emptyset$$

Докажем, что eK и $(1 - e)K$ – подкольца в K .

Признак подкольца:

$$\forall a, b \in S \quad (a - b) \in S$$

$$\forall a, b \in S \quad (ab) \in S$$

Пусть $S = eK, a = ex_1, b = ex_2.$

$$a - b = e(x_1 - x_2) \in eK$$

$$ab = ex_1ex_2 = e^2x_1x_2 = e(ex_1x_2) \in eK$$

Пусть $S = (1 - e)K, a = (1 - e)x_1, b = (1 - e)x_2$.

$$a - b = x_1 - x_2 - e(x_1 - x_2) = (1 - e)(x_1 - x_2) \in (1 - e)K$$

$$ab = (1 - e)x_1(1 - e)x_2 = (1 - e)((1 - e)x_1x_2) \in (1 - e)K$$

$$eK + (1 - e)K = K - \text{докажем это:}$$

Пусть $x \in K$. Тогда $x = ex + (1 - e)x = ex + x - ex = x$.

Значит $K \subseteq eK + (1 - e)K$. Так как $eK, (1 - e)K \subseteq K$, то $eK + (1 - e)K = \{ex + (1 - e)y = ex + y - ey | x, y \in K\} \subseteq K$.

Убедимся в том, что $eK \cap (1 - e)K = \{0\}$.

Пусть $a \in eK \cap (1 - e)K$. Тогда $\exists x, y \in K$ такие, что

$$a = ex = (1 - e)y$$

$$ea = e(ex) = e(1 - e)y = e(y - ey) = ey - ey = 0 \Rightarrow a = 0$$

Обозначим $eK + (1 - e)K = eK \oplus (1 - e)K$ – прямая сумма двух подколец.

Таким образом: $K = eK \oplus (1 - e)K$ является пирсовским разложением кольца K по идемпотенту e . Легко видеть, что $\forall a \in eK \quad ea = a$, то есть e – единичный элемент в подкольце eK . Аналогично: $\forall c \in (1 - e)K \quad ec = 0$. Значит, если $x \in eK$, а $y \in (1 - e)K$, то $e(x + y) = x \Rightarrow xy = 0$.

Пусть K – некоммутативное кольцо, e – идемпотентный элемент. Тогда, если e – не единица, то имеет место двустороннее пирсовское разложение:

$$K = eKe \oplus eK(1 - e) \oplus (1 - e)Ke \oplus (1 - e)K(1 - e).$$

ГЛАВА II. Система компьютерной алгебры GAP

2.1. *Общая характеристика пакета GAP*

Система компьютерной алгебры GAP, название которой расшифровывается как "Groups, Algorithms and Programming", была задумана около 30 лет назад как инструмент комбинаторной теории групп – раздела алгебры, изучающего группы, заданные порождающими элементами и определяющими соотношениями. С каждым новым обновлением программа значительно усовершенствовалась и охватывала все новые и новые разделы алгебры, и сейчас можно говорить, что она охватывает все разделы алгебры. GAP наиболее интересен для исследований в области абстрактной алгебры.

Данная программа значительно облегчает работу вычислений чисел, как целых, так и рациональных. Ограничения на эти числа программой не установлены, однако они будут вычислены на столько, насколько хватит памяти устройства, на котором будет запущена программа. Так же, система работает с конечными полями, многочленами от многих переменных, рациональными функциями, векторами и матрицами. И это лишь меньшая часть того, что можно реализовать в данной программе. Простейшие примеры задач представлены на официальном сайте GAP, где подробно описано действие программ.

Группы могут быть заданы в различной форме, например, как группы подстановок, матричные группы, группы, заданные порождающими элементами и определяющими соотношениями. Функции для работы с группами включают определение порядка группы, вычисление классов сопряженных элементов. Для ряда конечных групп доступно определение их типа изоморфизма. В системе могут быть определены векторные пространства над всеми доступными полями.

Существует графический интерфейс XGAP, который позволяет, например, графически изобразить решетку подгрупп группы.

Основные особенности GAP:

- язык программирования, довольно схожий с языком программирования Pascal;
- стандартные типы основных алгебраических объектов: групп (подстановок, абстрактных, матричных), колец, полей;
- удобные типы переменных, в том числе. оперативно изменяемые списки и записи;
- более 4 тысяч библиотечных функций;
- обширная библиотека данных, включая практически все группы, порядок которых не превосходит 1000;
- подробное и удобное описание (около 1600 стр.) в формате «гипертекст»;
- бесплатное получение по сети Internet вместе с исходными текстами, являющимися незаменимым наглядным пособием для освоения GAP;
- работа в большом количестве известных и наиболее встречающихся операционных систем, таких как DOS, Windows, Unix, Linux, MacOS;
- работа с процессором типа 386 и выше с ОЗУ от 8 Mb;
- занимаемое место на диске - от 10 до 100 Mb в зависимости от объема инсталляции;
- способность работать с ОЗУ до 128 Mb и файлом подкачки до 128 Mb.

В ходе выполнения работы, мною было опробовано несколько различных версий программ. Делалось это с целью сравнения удобства использования, скорости обработки данных и возможностей, которые расширяются с каждой новой версией программы. Для задач, поставленных мной в данной работе, не было необходимости использовать самые новые версии, поэтому я

использовала версию 4.3, которая установлена на большинство компьютеров, за которыми я делала запуск составленных программ.

2.2. Общие команды пакета

Как у любого языка программирования, у GAP есть свои ключевые слова, которые применяются при составлении алгоритмов. Вот некоторые из них: and, do, elif, else, end, if, fi, for, function, if, in, local, mod, not, do, od, or, repeat, return, then, until, while, quit, QUIT, break, rec, continue. Это простейшие команды, поэтому мы их называем ключевыми словами, но каждое из данных слов записывается по своему правилу, соответствующему GAP.

Далее приведен список основных специфических команд системы, используемые в программах данной работы (те команды, которые не вошли в список, будут описаны в тексте самой программы):

Таблица №1

Текст программы	Описание программы
MatAlgebra(GF(n),m)	# Построение алгебры матриц порядка m над полем, состоящим из n элементов
Elements(A)	# Элементы множества A
Dimension(A)	# Размерность алгебры A
Subalgebra(A,[m])	# Создание подалгебры алгебры A , порожденной элементом m
<u>Работа со списками и множествами:</u> N:=[]	# Создание пустого множества N
Size(N)	# Количество элементов множества N
AddSet(N,m)	# Присоединение элемента m к множеству N
Position(N,m)	# Порядок элемента m в списке N

IsSubsetSet(N,M)	# Проверяет, содержится ли каждый элемент множества M во множестве N
IntersectSet(N,M)	# Пересекает множество N с множеством M
UniteSet(N,M)	#Объединение множества N с множеством M
SubtractSet(N,M)	# Вычитает множество M от множества N , т.е. удаляет из множества M все элементы множества N
<u>Условный оператор:</u> if Q1 then P1; fi;	# Если $Q1$ - истина, то выполняется команда $P1$
if Q1 then P1; elif Q2 then A2; fi;	# Если $Q1$ - истина, то выполняется команда $P1$, а если $Q2$ - истина, то выполняется команда $P2$
<u>Работа с циклами:</u> for a in N do P; od;	# Для всех элементов множества N выполняется команда P
for i in [1..m] do P; od;	# Выполнение команды P m раз
<u>Работа с данными:</u> PrintTo(“***.dan”, N)	# Записывает данные в файл
Read(“***.dan”)	# Читает файл
quit;	# Выход из программы

Программы в данной таблице написаны схематично, поэтому подставляя в любую из программ необходимые значения, мы получим решения.

2.3. Команды для вычислений в алгебрах

Пусть F – поле и A – алгебра над F (кратко: A – F -алгебра). Все алгебры в GARe ассоциативны, это значит, что операция умножения в них ассоциативна.

Любая алгебра всегда содержит нулевой элемент, который может быть получен, вычитанием произвольного элемента из самого себя. Элементы поля F не рассматриваются как элементы A . Практическим обоснованием (очевидно и математическим тоже) для этого служит то, что даже если единичная матрица содержится в матричной алгебре A , все равно невозможно записать $1 + a$ для суммы единичной матрицы и элемента a алгебры A , так как независимо от алгебры A в GAPe уже определено это значение как прибавление 1 ко всем позициям матрицы a . Вместо этого необходимо писать

$\text{One}(A) + a$ или $a^0 + a$.

Родительские алгебры и подалгебры

GAP различает алгебры и подалгебры алгебр. Каждая подалгебра принадлежит уникальной основной алгебре, которую называют родителем подалгебры. Родительская алгебра – собственный родитель. Родительские алгебры конструируются при помощи операторов `Algebra` и `UnitalAlgebra`, подалгебры конструируются при помощи операторов `Subalgebra` и `UnitalSubalgebra`. Родитель первого аргумента оператора `Subalgebra` будет родителем созданной подалгебры. Алгебраические действия, совершаемые более, чем с одной алгеброй, предполагают, что аргументы имеют общего родителя. Возьмем, например, `Centralizer`. В этом случае должно быть два аргумента: алгебра A и алгебра B , где A родительская алгебра и B – подалгебра этой родительской алгебры, или A и B – подалгебры общей родительской алгебры P . В этих случаях `Centralizer` выдает централизатор B в A , который представлен как подалгебра общей родительской алгебры алгебр A и B . Заметим, что подалгебра родительской алгебры не должна быть собственной подалгеброй. Исключением этому правилу является теоретико-множественная функция `Intersection`, которая позволяет рассматривать пересечения алгебры с различными родительскими алгебрами. Всякий раз, когда имеется две подалгебры, которые имеют различные родительские алгебры, но имеют и общую супералгебру A , можно использовать `AsSubalgebra` или

AsUnitalSubalgebra для того, чтобы создать новые подалгебры, которые имеют общую родительскую алгебру A .

Теоретико-множественные функции для алгебр

Все теоретико-множественные функции, например, Intersection и Size могут быть применены к алгебрам, так как они являются областями. Все теоретико-множественные функции, не упомянутые здесь, не трактуются специально для алгебр.

Elements(A) вычисляет элементы алгебры A с использованием алгоритма Dimino. Заданная по умолчанию для алгебр функция вычисляет базис линейного пространства в то же самое время.

Intersection(A, H) выдает пересечение A и H в виде множества элементов или как алгебраическую запись (запись алгебры).

IsSubset (A, H)

Если A и H – алгебры, то IsSubset проверяет являются ли генераторы H элементами A . Другой способ состоит в применении DomainOps.IsSubset.

Random(A) выдает произвольный элемент алгебры A . Это требует вычисления базиса линейного пространства.

Проверка свойств алгебр

С помощью GAPa могут быть проверены следующие свойства алгебр.

IsAbelian(A) выдается true если алгебра A абелева и false в противном случае. Алгебра A называется абелевой, если и только, если для любых $a, b \in A$ $a*b = b*a$.

IsCentral(A, U) выдается true если алгебра A централизует алгебру U и false в противном случае. Алгебра A централизует алгебру U , если и только, если для всякого $a \in A$ и для всякого $u \in U$ $a*u = u*a$. Заметьте, что U не обязана быть подалгеброй A , но они должны иметь общую родительскую алгебру.

`IsFinite(A)` выдается `true` если алгебра A конечна, и `false` в противном случае.

`IsTrivial(A)` выдается `true` если алгебра A состоит только из нулевого элемента, и `false` в противном случае. Если A — унитарная алгебра, то, конечно, она никогда не тривиальна.

Все критерии ожидают родительскую алгебру или подалгебру и выдают `true`, если алгебра имеет свойство и `false` в противном случае. Некоторые функции не могут выполняться, если данная алгебра имеет бесконечное множество элементов. В таких случаях может быть напечатано предупреждение.

Функции линейного пространства для алгебр

Конечномерная F — алгебра A всегда есть конечномерное векторное пространство над F . Таким образом, в GAPe, алгебра — линейное пространство, и функции линейного пространства типа `Base` и `Dimension` применимы к алгебрам.

Структура линейного пространства используется также теоретико-множественными функциями.

ГЛАВА III. Типовая классификация подалгебр четырёхмерной алгебры матриц $M(GF(2),3)$

3.1. *Подалгебры четырёхмерной алгебры матриц над полем из двух элементов*

В данной работе были составлены программы с умножениями порождающих элементов. Эти программы запускаем в GAP. Ниже приведена одна из них:

Таблица 2

Текст программы	Комментарии
Sub:=[];	Создание массива
RRE:=[];	Создание массива
b:=0;	Обнуление элемента b
RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR
ID:=[2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка над полем

	GF(2)
El:=Elements(A);	Создание массива элементов алгебры A
for i in RR do	Начало цикла
for k in ID do	Начало цикла
B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	Записывает подалгебру алгебры A, порожденную элементами [El[i[1]],El[i[2]],El[k]]
if Size(B)=16 then	Конец цикла
if El[k]*El[i[1]]=El[i[1]] and El[i[1]]*El[k]=El[i[1]] and El[k]*El[i[2]]=El[i[2]] and El[i[2]]*El[k]=El[i[2]] then	Таблица умножения из Пирсовского разложения
sub:=Elements(B);	Нахождение всех матриц
AddSet(Sub,sub);	Запись в массив Sub
if Size(Sub) > b then	Проверим размер массива Sub
Add(RRE,[i[1],i[2],k]);	Запись массива
b:=Size(Sub);	Задание размера массива
fi;fi;fi;	Заккрытие всех циклов

od; od;	Конец цикла в цикле; конец цикла
Sort(RRE);	Сортировка массива
PrintTo("4ER1=R1_R1E=R1_R2E=R2=ER2.dan","RRE:= ",RRE,";", "\n", " RRE =", Size(RRE), "\n", "Sub1:=", Sub, ";", "\n");	Вывод на экран

Данная программа находит номера всех троек элементов, порождающих подалгебры с заданной таблицей умножения. Результат работы программы содержится в файле «4ER1=R1_R1E=R1_R2E=R2=ER2.dan» и выглядит следующим образом:

```
RRE:= [ [ 13, 5, 274 ], [ 32, 5, 274 ], [ 35, 33, 274 ], [ 67, 3, 274 ],
[ 79, 7, 274 ], [ 92, 28, 274 ], [ 97, 65, 274 ], [ 120, 64, 274 ],
[ 133, 129, 274 ], [ 137, 9, 274 ], [ 171, 41, 274 ], [ 190, 64, 274 ],
[ 222, 7, 274 ], [ 229, 193, 274 ], [ 244, 41, 274 ], [ 328, 3, 274 ],
[ 334, 326, 274 ], [ 375, 28, 274 ], [ 435, 433, 274 ], [ 441, 9, 274 ],
[ 477, 456, 274 ] ];
|RRE|=21
```

Далее рассмотрим любую из этих троек. Для примера возьмем первую тройку: [13, 5, 274] и найдем тип решетки подалгебр алгебры, порожденной данной тройкой.

3.2. *Вычисление типа подалгебры*

Определение 7. Пусть S подалгебра порядка 2^n алгебры $M_3(GF(2))$. Назовем упорядоченную последовательность (m_0, m_1, \dots, m_n) типом решетки подалгебр алгебры A , если m_i – число подалгебр в A порядка 2^i .

Для того, чтобы вычислить тип решетки, была составлена следующая программа:

Таблица 3

Программа №2	
tip:=function(a,b,c)	Задаем функцию
Local	Создаем локальные переменные
A, El, i, j, k, sub, tip, S, s, el, l;	Имена переменных
sub:=[];	Задаем пустой массив sub
tip:=[];	Задаем пустой массив tip
A:=MatAlgebra(GF(2),3);	Создание алгебры матриц
El:=Elements(A);	Построение массива элементов
S:=Subalgebra(A,[El[a],El[b],El[c]]);	Построение подалгебры
for i in S do	Начало цикла
for k in S do	Начало цикла
for j in S do	Начало цикла
s:=Subalgebra(A,[i,j,k]);	Построение подалгебры
AddSet(sub,Elements(s));	Построение массива элементов и добавление его в массив sub
od;	Закрытие цикла
od;	Закрытие цикла
od;	Закрытие цикла
for l in [1..Size(sub)] do	Начало цикла
Add(tip,Size(sub[l]));	Добавление порядка каждого элемента в массив tip
od;	Закрытие цикла
tip:=Collected(tip);	Считаем количество элементов каждого порядка и сохраняем их в tip
PrintTo("tip.txt","a= ",a,";", " b= ",b,";", " c= ",c,";", "\n",tip);	Распечатываем результаты в файл tip.txt
end;;	Конец функции

Замечание. Некоторые программы, используемые в данной работе, используют одни и те же данные, поэтому все файлы желательно поместить в ту директорию, в которой будет запускаться программа.

Пояснения к использованию программы

Для запуска программы необходимо набрать в среде GAP команду:

$$\text{tip}(a, b, c);,$$

взяв тройку из массива $\text{Gen}(n)$, где $n \in \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Пример, поясняющий запуск программы и ее работу:

Запустим программу, набрав $\text{tip}(13, 5, 274);$. Распечатаем файл `tip.txt`.

Результат имеет вид:

$a= 13; b= 5; c= 274;$

$[[1, 1], [2, 6], [4, 8], [8, 4], [16, 1]]$

Объясним, что означает это строка.

$[1, 1]$ – одна подалгебра порядка 1, то есть нулевая подалгебра;

$[2, 6]$ – 6 подалгебр порядка 2;

$[4, 8]$ – 8 подалгебр порядка 4;

$[8, 4]$ – 4 подалгебры порядка 8;

$[16, 1]$ – 1 подалгебра порядка 16.

Полученную последовательность пар можно переписать и в таком виде:

$$(1, 6, 8, 4, 1).$$

Это и есть тип подалгебры, порожденной матрицами с номерами 13, 5, 274.

3.3. Определение отношения покрытия

Далее, исследуем отношение покрытия в решетке подалгебр:

Таблица 4

Программа №3

пок:=function(a,b,c)	Задание функции
local	Задание переменных
A, El, i, j, k, sub, tip, S, s, s1, el, l, l1, m, m1, n, n1, i1;	Имена переменных
sub:=[];	Создаем массив sub
for i1 in [1..9] do	Начало цикла
sub[i1]:=[];	Создаем в массиве sub 9 пустых массивов
od;	Конец цикла
пок:=[];	Создание массива пок
A:=MatAlgebra(GF(2),3);	Создание алгебры
El:=Elements(A);	Построение массива элементов
S:=Subalgebra(A,[El[a],El[b],El[c]]);	Записывает подалгебру алгебры A порожденную элементами El[a],El[b],El[c] в S
for i in S do	Начало цикла
for k in S do	Начало цикла
for j in S do	Начало цикла
s1:=Subalgebra(S,[i,k,j]);	Записывает подалгебру алгебры S порожденную элементами i,k,j в s1
if Size(s1)=1 then	Проверяем размер. Если равен 1
AddSet(sub[1],Elements(s1));	Записываем в 1-й массив
fi;	Закрываем проверку условия
if Size(s1)=2 then	Если равен 2
AddSet(sub[2],Elements(s1));	Записываем во 2-й массив
fi;	Закрываем проверку условия

if Size(s1)=4 then	Если равен 4
AddSet(sub[3],Elements(s1));	Записываем в 3-й массив
fi;	Закрываем проверку условия
if Size(s1)=8 then	Если равен 8
AddSet(sub[4],Elements(s1));	Записываем в 4-й массив
fi;	Закрываем проверку условия
if Size(s1)=16 then	Если равен 16
AddSet(sub[5],Elements(s1));	Записываем в 5-й массив
fi;	Закрываем проверку условия
if Size(s1)=32 then	Если равен 32
AddSet(sub[6],Elements(s1));	Записываем в 6-й массив
fi;	Закрываем проверку условия
if Size(s1)=64 then	Проверяем размер. Если равен 64
AddSet(sub[7],Elements(s1));	Записываем в 7-й массив
fi;	Закрываем проверку условия
if Size(s1)=128 then	Если равен 128
AddSet(sub[8],Elements(s1));	Записываем в 8-й массив
fi;	Закрываем проверку условия
if Size(s1)=512 then	Проверяем размер. Если равен 512
AddSet(sub[9],Elements(s1));	Записываем в 9-й массив
fi;	Закрываем проверку условия
od;	Заккрытие цикла
od;	Заккрытие цикла
od;	Заккрытие цикла
for m1 in [1..Size(sub)] do	Открытие цикла
for l1 in [1..Size(sub[m1])] do	Открытие цикла
for n1 in [1..Size(sub[m1+1])] do	Открытие цикла
if IsSubset(sub[m1+1][n1],sub[m1][l1])=true	Проверяет являются ли генераторы sub[m1][l1] элементами sub[m1+1][n1],
Then Add(pokr,[m1,l1],[m1+1,n1]);	если да, то записывает в pokr
fi;	Заккрытие проверки условия
od;	Конец цикла
od;	Конец цикла

od;	Конец цикла
PrintTo("pokr.txt", pokr, "\n");	Распечатываем массив pokr
end;;	Конец функции

Результатом работы программы является следующий список покрытий:

```

[[ [ 1, 1 ], [ 2, 1 ] ], [ [ 1, 1 ], [ 2, 2 ] ], [ [ 1, 1 ], [ 2, 3 ] ],
[ [ 1, 1 ], [ 2, 4 ] ], [ [ 1, 1 ], [ 2, 5 ] ], [ [ 1, 1 ], [ 2, 6 ] ],
[ [ 2, 1 ], [ 3, 1 ] ], [ [ 2, 1 ], [ 3, 2 ] ], [ [ 2, 2 ], [ 3, 3 ] ],
[ [ 2, 2 ], [ 3, 4 ] ], [ [ 2, 3 ], [ 3, 1 ] ], [ [ 2, 3 ], [ 3, 3 ] ],
[ [ 2, 3 ], [ 3, 5 ] ], [ [ 2, 3 ], [ 3, 6 ] ], [ [ 2, 4 ], [ 3, 1 ] ],
[ [ 2, 4 ], [ 3, 7 ] ], [ [ 2, 5 ], [ 3, 3 ] ], [ [ 2, 5 ], [ 3, 8 ] ],
[ [ 2, 6 ], [ 3, 2 ] ], [ [ 2, 6 ], [ 3, 4 ] ], [ [ 2, 6 ], [ 3, 6 ] ],
[ [ 2, 6 ], [ 3, 7 ] ], [ [ 2, 6 ], [ 3, 8 ] ], [ [ 3, 1 ], [ 4, 1 ] ],
[ [ 3, 1 ], [ 4, 2 ] ], [ [ 3, 2 ], [ 4, 2 ] ], [ [ 3, 3 ], [ 4, 1 ] ],
[ [ 3, 3 ], [ 4, 3 ] ], [ [ 3, 4 ], [ 4, 3 ] ], [ [ 3, 5 ], [ 4, 1 ] ],
[ [ 3, 5 ], [ 4, 4 ] ], [ [ 3, 6 ], [ 4, 2 ] ], [ [ 3, 6 ], [ 4, 3 ] ],
[ [ 3, 6 ], [ 4, 4 ] ], [ [ 3, 7 ], [ 4, 2 ] ], [ [ 3, 8 ], [ 4, 3 ] ],
[ [ 4, 1 ], [ 5, 1 ] ], [ [ 4, 2 ], [ 5, 1 ] ], [ [ 4, 3 ], [ 5, 1 ] ],
[ [ 4, 4 ], [ 5, 1 ] ] ]

```

Объясним, как прочесть полученную информацию. В данном примере рассматривается подалгебра, порожденная матрицами с номерами 13, 5 и 274. Эта подалгебра содержит 16 элементов и имеет тип (1, 6, 8, 4, 1) одна нулевая подалгебра, 6 двухэлементных, 8 четырехэлементных, 4 восьмиэлементных, одна шестнадцатиэлементная подалгебра. Таким образом, все подалгебры в решетке подалгебр алгебры распределены по пяти уровням. На каждом уровне алгебры имеют двойные номера, например, номер [3, 9] означает, что 3 – номер уровня, а 9 – порядковый номер подалгебры на третьем уровне. Таким образом, запись [[3, 9], [4, 7]] означает, что подалгебра с номером [3, 9] покрывается подалгеброй с номером [4, 7] в решетке подалгебр.

3.4. Построение диаграммы решетки

Используя полученную информацию, построим диаграмму решетки подалгебр алгебры S . Построение осуществим в несколько этапов.

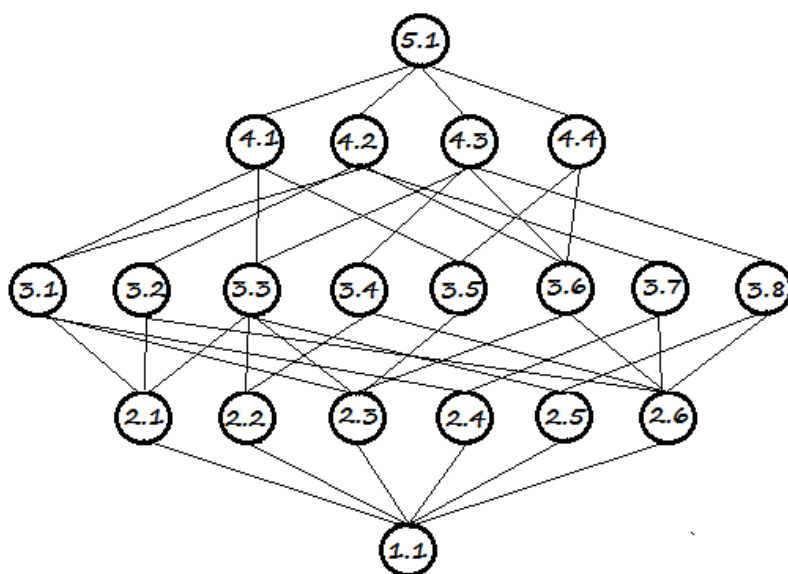
- 1) Изобразим подалгебры алгебры S кружочками.
- 2) Изобразим отношение покрытия, соединяя покрываемый элемент с покрывающим отрезком.

В результате имеем решетку:

Рис.1

Из проведенных вычислений вытекает следующая теорема:

Теорема 2. Все 21 подалгебры типа $(1, 6, 8, 4, 1)$ изоморфны между собой,



а значит подалгебры типа $(1, 6, 8, 4, 1)$ имеют изоморфные решетки подалгебр.

Аналогичные исследования проводятся для подалгебр, имеющих другие таблицы умножения.

Составляем новую программу с новым умножением:

Таблица 5

Программа №3	
Текст программы	Комментарии

Sub:=[];	Создание массива
RRE:=[];	Создание массива
b:=0;	Обнуление элемента b
RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR
ID:=[2, 4, 6, 8, 1, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 21, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка над полем GF(2)
El:=Elements(A);	Создание массива элементов алгебры A
for i in RR do	Проверка
for k in ID do	Проверка
B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	
if Size(B)=16 then	Конец цикла
if El[k]*El[i[1]]=El[i[1]] and El[i[1]]*El[k]=El[i[1]]+El[i[2]] and El[k]*El[i[2]]=El[i[2]] and El[i[2]]*El[k]=El[1] then	Таблица умножения из Пирсовского разложения
sub:=Elements(B);	Нахождение всех матриц
AddSet(Sub,sub);	Запись в массив Sub
if Size(Sub) > b then	Проверяем размер массива Sub
Add(RRE,[i[1],i[2],k]);	Добавляем в массив RRE элементы i[1],i[2],k

b:=Size(Sub);	Находим число всех матриц
fi;fi;fi;	Закрытие всех циклов
od; od;	Конец цикла в цикле; конец цикла
Sort(RRE);	Сортировка массива RRE
PrintTo("4ER1=R1_R1E=R1+R2_R2E=0_ER2=R2.dan","RRE:=",RRE,";","\n"," RRE =",Size(RRE),"\n","Sub2:=",Sub,";","\n");	Вывод на экран

Результат работы программы выглядит следующим образом:
RRE:= [[13, 5, 18], [32, 5, 18], [35, 33, 18], [67, 3, 258],
[79, 7, 146], [92, 28, 266], [97, 65, 273], [120, 64, 21],
[133, 129, 258], [137, 9, 273], [171, 41, 82], [190, 64, 21],
[222, 7, 146], [229, 193, 266], [244, 41, 82], [328, 3, 258],
[334, 326, 82], [375, 28, 266], [435, 433, 146], [441, 9, 273],
[477, 456, 21]];
|RRE|=21.

Остальные программы и результаты их работы, задающие умножения, представлены в приложениях 3-7.

В этой программе, как и в предыдущей, получилась 21 тройка, удовлетворяющая заданному умножению. Из этих троек точно так же выберем только одну, так как в теореме 2 сказано, что все тройки будут изоморфны, а значит, будут иметь один и тот же тип, покрытие и диаграмму.

По программе 2 исследуем тип: [[1, 1], [2, 9], [4, 13], [8, 4], [16, 1]] – результат программы. Преобразуем в удобную форму: тип- (1, 9, 13, 4, 1).

По программе 3 исследуем покрытие:

[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]],
[[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]],
[[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]],
[[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]],
[[2, 2], [3, 4]], [[2, 2], [3, 5]], [[2, 2], [3, 6]],

$[[2, 3], [3, 1]], [[2, 3], [3, 4]], [[2, 3], [3, 8]],$
 $[[2, 3], [3, 9]], [[2, 4], [3, 1]], [[2, 4], [3, 10]],$
 $[[2, 4], [3, 11]], [[2, 4], [3, 12]], [[2, 5], [3, 2]],$
 $[[2, 5], [3, 5]], [[2, 5], [3, 7]], [[2, 5], [3, 8]],$
 $[[2, 5], [3, 10]], [[2, 6], [3, 2]], [[2, 6], [3, 9]],$
 $[[2, 6], [3, 11]], [[2, 7], [3, 5]], [[2, 7], [3, 12]],$
 $[[2, 7], [3, 13]], [[2, 8], [3, 3]], [[2, 8], [3, 6]],$
 $[[2, 8], [3, 8]], [[2, 8], [3, 11]], [[2, 9], [3, 3]],$
 $[[2, 9], [3, 9]], [[2, 9], [3, 10]], [[2, 9], [3, 13]],$
 $[[3, 1], [4, 2]], [[3, 2], [4, 1]], [[3, 2], [4, 2]],$
 $[[3, 3], [4, 2]], [[3, 4], [4, 3]], [[3, 5], [4, 1]],$
 $[[3, 5], [4, 3]], [[3, 5], [4, 4]], [[3, 6], [4, 3]],$
 $[[3, 7], [4, 1]], [[3, 8], [4, 2]], [[3, 8], [4, 3]],$
 $[[3, 9], [4, 2]], [[3, 10], [4, 2]], [[3, 10], [4, 4]],$
 $[[3, 11], [4, 2]], [[3, 12], [4, 4]], [[3, 13], [4, 4]], [[4, 1], [5, 1]],$
 $[[4, 2], [5, 1]], [[4, 3], [5, 1]],$
 $[[4, 4], [5, 1]]]$

И по тем же правилам рисуем диаграмму решетки (Рис. 2).

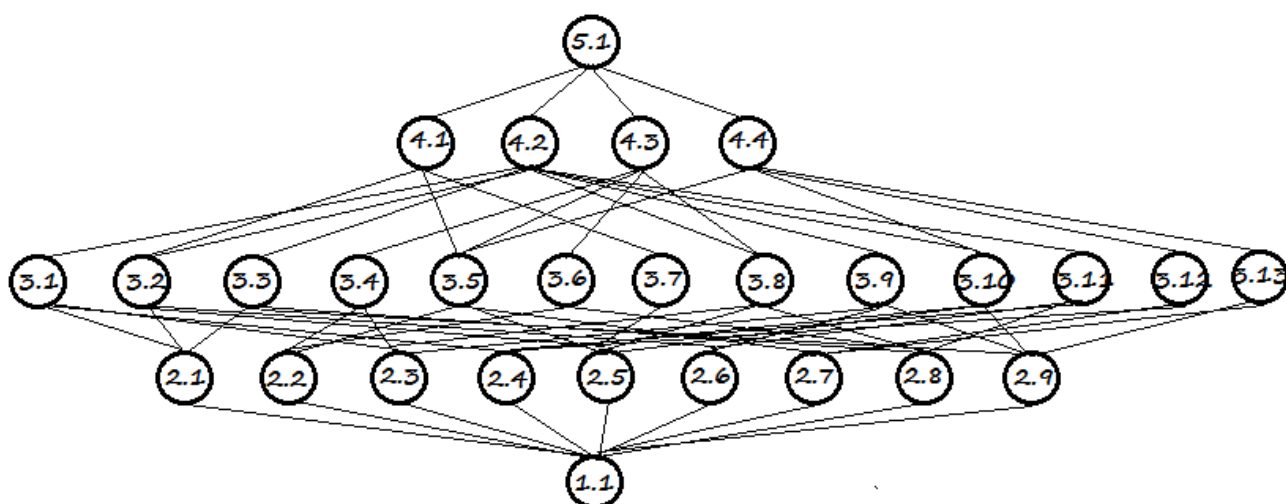


Рис.2

Приведем подпрограммы, вставляемые в основную программу, для определения новых таблиц умножения в подалгебрах.:

Таблица 6

Умножение	Количество найденных троек	Выбранная тройка	Тип
if $El[k]*El[i[1]]=El[i[1]]$ and $El[i[1]]*El[k]=El[i[1]]$ and $El[k]*El[i[2]]=El[i[2]]$ and $El[i[2]]*El[k]=El[i[2]]$ then	21	[13, 5, 274]	(1, 6 ,8, 4, 1)
if $El[k]*El[i[1]]=El[i[1]]$ and $El[i[1]]*El[k]=El[i[1]]+El[i[2]]$ and $El[k]*El[i[2]]=El[i[2]]$ and $El[i[2]]*El[k]=El[1]$ then	21	[13, 5, 18]	(1, 9, 13, 4, 1).

if $El[k]*El[i[1]]=El[i[1]]+El[i[2]]$ and $El[i[1]]*El[k]=El[i[2]]$ and $El[k]*El[i[2]]=El[1]$ and $El[i[2]]*El[k]=El[i[2]]$ then	21	[13, 5, 273]	(1, 9, 11, 5, 1)
if $El[k]*El[i[1]]=El[i[2]]$ and $El[i[1]]*El[k]=El[i[1]]$ and $El[k]*El[i[2]]=El[i[2]]$ and $El[i[2]]*El[k]=El[i[2]]$ then	21	[13, 5, 258]	(1, 9, 13, 4, 1)
if $El[k]*El[i[1]]=El[i[2]]$ and $El[i[1]]*El[k]=El[i[1]]$ and $El[k]*El[i[2]]=El[i[2]]$ and $El[i[2]]*El[k]=El[i[2]]$ then	21	[13, 5, 17]	(1,9,13,4,1)
if $El[k]*El[i[1]]=El[i[2]]$ and $El[i[1]]*El[k]=El[i[1]]+El[i[2]]$ and $El[k]*El[i[2]]=El[i[2]]$ and $El[i[2]]*El[k]=El[1]$ then	21	[13, 5, 2]	(1,9,11,5,1)
if $El[k]*El[i[1]]=El[1]$ and $El[i[1]]*El[k]=El[i[2]]$ and $El[k]*El[i[2]]=El[1]$ and $El[i[2]]*El[k]=El[i[2]]$ then	21	[13, 5, 257]	(1,9,13,4,1)

Из составленной таблицы можно заметить, что различным тройкам может соответствовать один и тот же тип. Тогда стоит задача выяснить будут ли одинаковыми решетки подалгебр с одинаковым типом. Для этого продолжим исследования каждой тройки и определим их покрытия для того, чтобы в дальнейшем можно было изобразить решетки. Эти исследования представлены в таблице 7. Покрытия посчитаны по ранее созданной программе №3 из таблицы 4.

Таблица 7

[illegible]

			3, 5], [4, 1]], [[3, 5], [4, 3]], [[3, 5], [4, 4]], [[3, 6], [4, 3]], [[3, 7], [4, 1]], [[3, 8], [4, 2]], [[3, 8], [4, 3]], [[3, 9], [4, 2]], [[3, 10], [4, 2]], [[3, 10], [4, 4]], [[3, 11], [4, 2]], [[3, 12], [4, 4]], [[3, 13], [4, 4]], [[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]]]
№3	[13, 5, 273]	(1, 9, 11, 5, 1)	[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]], [[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]], [[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]], [[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 2], [3, 3]], [[2, 2], [3, 4]], [[2, 3], [3, 1]], [[2, 3], [3, 3]], [[2, 3], [3, 5]], [[2, 3], [3, 6]], [[2, 3], [3, 7]], [[2, 3], [3, 8]], [[2, 3], [3, 9]], [[2, 4], [3, 1]], [[2, 4], [3, 10]], [[2, 5], [3, 3]], [[2, 5], [3, 11]], [[2, 6], [3, 2]], [[2, 6], [3, 4]], [[2, 6], [3, 6]], [[2, 7], [3, 2]], [[2, 7], [3, 7]], [[2, 7], [3, 11]], [[2, 8], [3, 4]], [[2, 8], [3, 8]], [[2, 8], [3, 10]], [[2, 9], [3, 9]], [[2, 9], [3, 10]], [[2, 9], [3, 11]], [[3, 1], [4, 1]], [[3, 1], [4, 2]], [[3, 1], [4, 3]], [[3, 2], [4, 2]], [[3, 3], [4, 1]], [[3, 3], [4, 4]], [[3, 3], [4, 5]], [[3, 4], [4, 4]], [[3, 5], [4, 1]], [[3, 6], [4, 2]], [[3, 6], [4, 4]], [[3, 7], [4, 2]], [[3, 7], [4, 5]], [[3, 8], [4, 3]], [[3, 8], [4, 4]], [[3, 9], [4, 3]], [[3, 9], [4, 5]], [[3, 10], [4, 3]], [[3, 11], [4, 5]], [[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]], [[4, 5], [5, 1]]]
№4	[13, 5, 258]	(1, 9, 13, 4, 1)	[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]], [[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]], [[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]], [[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 4]], [[2, 2], [3, 5]], [[2, 2], [3, 6]], [[2, 3], [3, 1]], [[2, 3], [3, 4]], [[2, 3], [3, 7]], [[2, 3], [3, 8]], [[2, 3], [3, 9]], [[2, 4], [3, 1]], [[2, 4], [3, 10]], [[2, 4], [3, 11]], [[2, 5], [3, 4]], [[2, 5], [3, 12]], [[2, 5], [3, 13]], [[2, 6], [3, 2]], [[2, 6], [3, 5]], [[2, 6], [3, 8]], [[2, 6], [3, 12]], [[2, 7], [3, 5]], [[2, 7], [3, 9]], [[2, 7], [3, 10]], [[2, 7], [3, 13]], [[2, 8], [3, 3]], [[2, 8], [3, 6]], [[2, 8], [3, 8]], [[2, 8], [3, 13]], [[2, 9], [3, 6]], [[2, 9], [3, 9]], [[2, 9], [3, 11]], [[2, 9], [3, 12]], [[3, 1], [4, 1]], [[3, 1], [4, 2]], [[3, 1], [4, 3]], [[3, 2], [4, 2]], [[3, 3], [4, 2]], [[3, 4], [4, 1]], [[3, 4], [4, 4]], [[3, 5], [4, 4]], [[3, 6], [4, 4]], [[3, 7], [4, 1]], [[3, 8], [4, 2]], [[3, 8], [4, 4]], [[3, 9], [4, 3]], [[3, 9], [4, 4]]]

			, [4, 4]], [[3, 10], [4, 3]], [[3, 11], [4, 3]], [[3, 12], [4, 4]], [[3, 13], [4, 4]], [[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]]]
№5	[13, 5, 17]	(1,9,13,4,1)	[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]], [[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]], [[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]], [[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 4]], [[2, 2], [3, 5]], [[2, 2], [3, 6]], [[2, 3], [3, 1]], [[2, 3], [3, 4]], [[2, 3], [3, 8]], [[2, 3], [3, 9]], [[2, 4], [3, 4]], [[2, 4], [3, 10]], [[2, 4], [3, 11]], [[2, 4], [3, 12]], [[2, 5], [3, 2]], [[2, 5], [3, 5]], [[2, 5], [3, 7]], [[2, 5], [3, 8]], [[2, 5], [3, 10]], [[2, 6], [3, 2]], [[2, 6], [3, 11]], [[2, 6], [3, 13]], [[2, 7], [3, 5]], [[2, 7], [3, 9]], [[2, 7], [3, 12]], [[2, 8], [3, 3]], [[2, 8], [3, 6]], [[2, 8], [3, 8]], [[2, 8], [3, 12]], [[2, 9], [3, 6]], [[2, 9], [3, 9]], [[2, 9], [3, 10]], [[2, 9], [3, 13]], [[3, 1], [4, 2]], [[3, 2], [4, 1]], [[3, 2], [4, 2]], [[3, 2], [4, 3]], [[3, 3], [4, 2]], [[3, 4], [4, 4]], [[3, 5], [4, 1]], [[3, 5], [4, 4]], [[3, 6], [4, 4]], [[3, 7], [4, 1]], [[3, 8], [4, 2]], [[3, 8], [4, 4]], [[3, 9], [4, 4]], [[3, 10], [4, 3]], [[3, 10], [4, 4]], [[3, 11], [4, 3]], [[3, 12], [4, 4]], [[3, 13], [4, 3]], [[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]]]
№6	[13, 5, 2]	(1,9,11,5,1)	[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]], [[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]], [[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]], [[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 1]], [[2, 2], [3, 4]], [[2, 3], [3, 1]], [[2, 3], [3, 5]], [[2, 3], [3, 6]], [[2, 4], [3, 2]], [[2, 4], [3, 7]], [[2, 5], [3, 2]], [[2, 5], [3, 8]], [[2, 5], [3, 9]], [[2, 6], [3, 3]], [[2, 6], [3, 4]], [[2, 6], [3, 5]], [[2, 6], [3, 7]], [[2, 6], [3, 8]], [[2, 6], [3, 10]], [[2, 6], [3, 11]], [[2, 7], [3, 4]], [[2, 7], [3, 9]], [[2, 8], [3, 6]], [[2, 8], [3, 7]], [[2, 9], [3, 6]], [[2, 9], [3, 9]], [[2, 9], [3, 11]], [[3, 1], [4, 1]], [[3, 2], [4, 2]], [[3, 3], [4, 1]], [[3, 3], [4, 2]], [[3, 4], [4, 1]], [[3, 4], [4, 3]], [[3, 4], [4, 4]], [[3, 5], [4, 1]], [[3, 5], [4, 5]], [[3, 6], [4, 5]], [[3, 7], [4, 2]], [[3, 7], [4, 3]], [[3, 7], [4, 5]], [[3, 8], [4, 2]], [[3, 8], [4, 4]], [[3, 9], [4, 4]], [[3, 10], [4, 3]], [[3, 11], [4, 4]], [[3, 11], [4, 5]], [[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4]]]

], [5, 1]], [[4, 5], [5, 1]]]
№7	[13, 5, 257]	(1,9,13,4,1)	[[[1, 1], [2, 1]], [[1, 1], [2, 2]], [[1, 1], [2, 3]], [[1, 1], [2, 4]], [[1, 1], [2, 5]], [[1, 1], [2, 6]], [[1, 1], [2, 7]], [[1, 1], [2, 8]], [[1, 1], [2, 9]], [[2, 1], [3, 1]], [[2, 1], [3, 2]], [[2, 1], [3, 3]], [[2, 2], [3, 4]], [[2, 2], [3, 5]], [[2, 2], [3, 6]], [[2, 3], [3, 1]], [[2, 3], [3, 4]], [[2, 3], [3, 7]], [[2, 3], [3, 8]], [[2, 3], [3, 9]], [[2, 4], [3, 1]], [[2, 4], [3, 10]], [[2, 4], [3, 11]], [[2, 5], [3, 4]], [[2, 5], [3, 12]], [[2, 5], [3, 13]], [[2, 6], [3, 2]], [[2, 6], [3, 5]], [[2, 6], [3, 8]], [[2, 6], [3, 10]], [[2, 7], [3, 2]], [[2, 7], [3, 9]], [[2, 7], [3, 11]], [[2, 7], [3, 12]], [[2, 8], [3, 3]], [[2, 8], [3, 6]], [[2, 8], [3, 8]], [[2, 8], [3, 11]], [[2, 9], [3, 3]], [[2, 9], [3, 9]], [[2, 9], [3, 10]], [[2, 9], [3, 13]], [[3, 1], [4, 1]], [[3, 1], [4, 2]], [[3, 2], [4, 2]], [[3, 3], [4, 2]], [[3, 4], [4, 1]], [[3, 4], [4, 3]], [[3, 4], [4, 4]], [[3, 5], [4, 3]], [[3, 6], [4, 3]], [[3, 7], [4, 1]], [[3, 8], [4, 2]], [[3, 8], [4, 3]], [[3, 9], [4, 2]], [[3, 9], [4, 4]], [[3, 10], [4, 2]], [[3, 11], [4, 2]], [[3, 12], [4, 4]], [[3, 13], [4, 4]], [[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]]]

Из этой таблицы мы можем задать классификацию четырехмерных подалгебр в алгебре матриц третьего порядка над полем из двух элементов. Можно заметить следующее: подалгебр с типом $(1, 6, 8, 4, 1)$ содержится только одна, с типом $(1, 9, 11, 5, 1)$ – две, с типом $(1, 9, 13, 4, 1)$ – четыре. Таким образом, перед нами стоит вопрос об изоморфизме решеток для каждого найденного типа. Создадим рисунки для каждого из типов подалгебр. Номера рисунков соответствуют номеру в таблице.

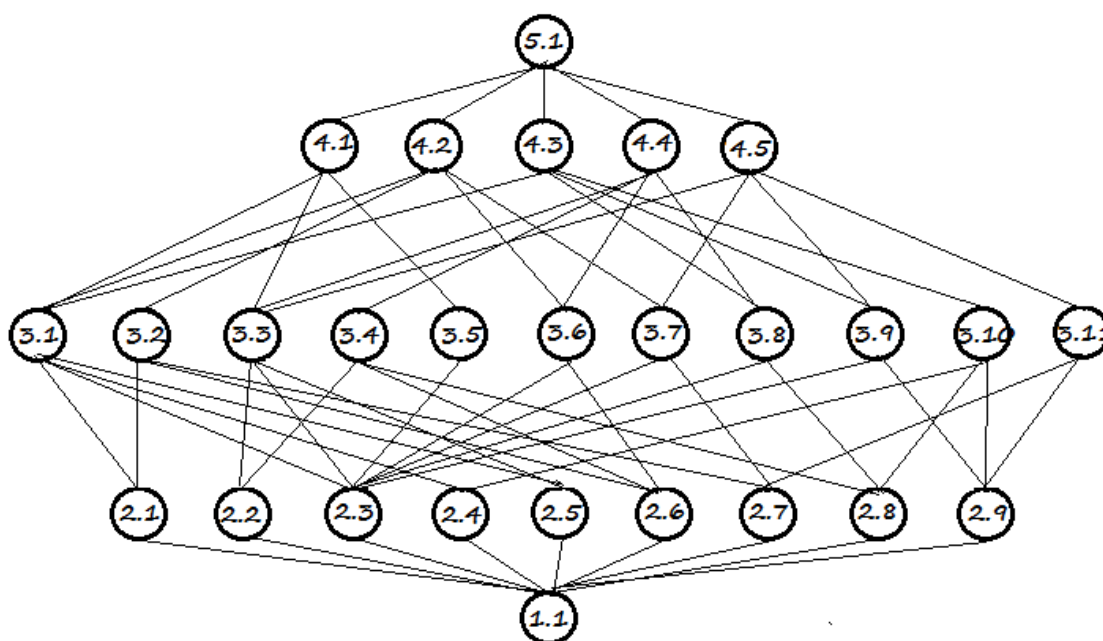
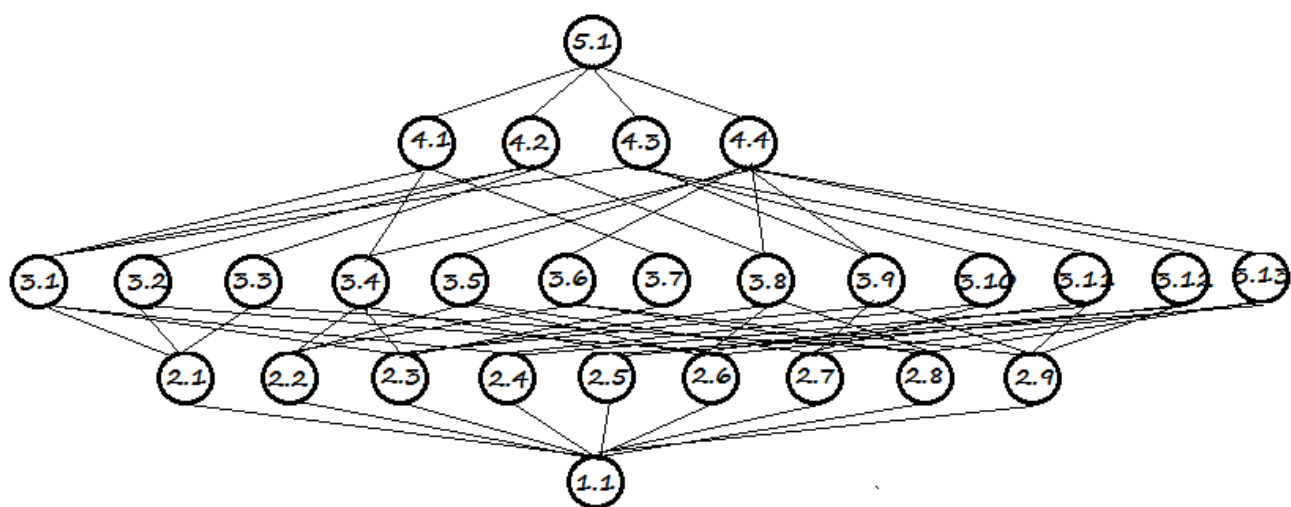
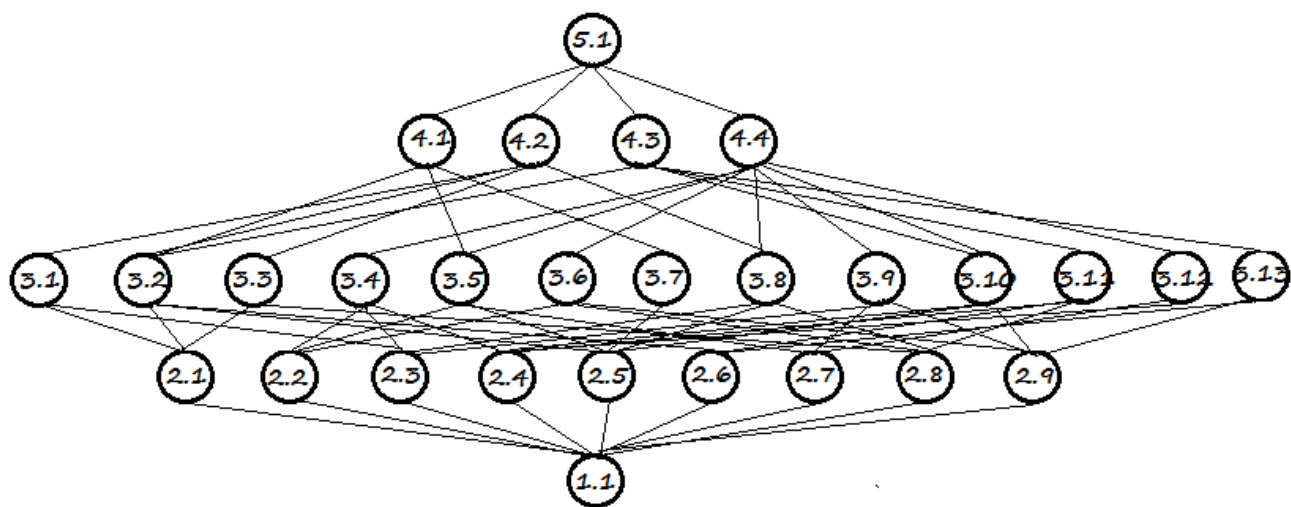


Рис. 3



Puc.4



Puc.5

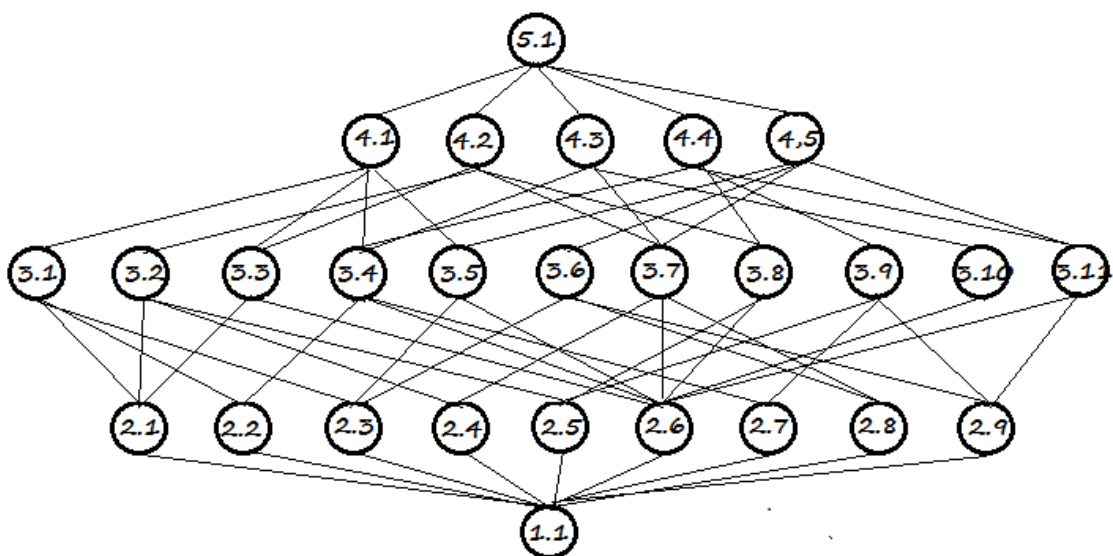


Рис.6

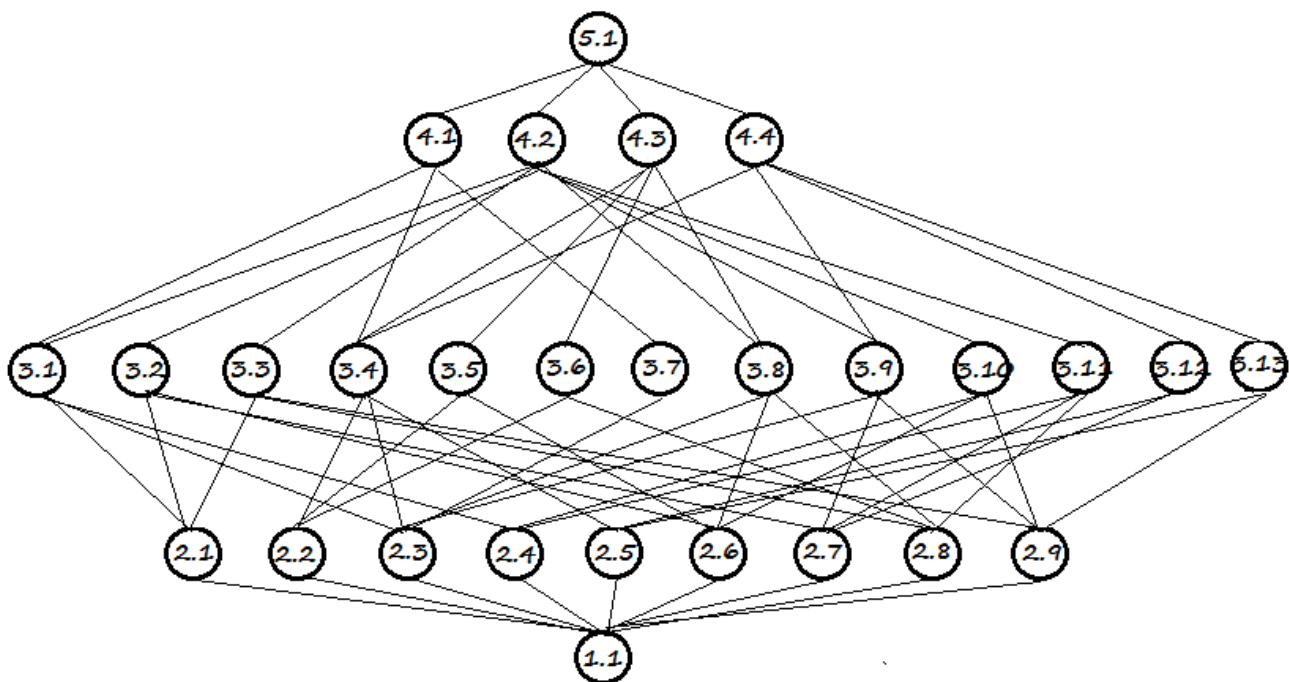


Рис.7

3.5. Типы решеток подалгебр четырехмерных подалгебр

Из ранее известных результатов [11], представленных в таблице 8, можно увидеть, что для выбранных нами типов решеток $(1,6,8,4,1)$, $(1,9,11,5,1)$, $(1,9,13,4,1)$ подалгебры найдены в полном объеме:

- (1,6,8,4,1) – 21 подалгебра в таблице 6 и 21 подалгебра в таблице 8;
 (1,9,11,5,1) – 42 подалгебры в таблице 6 и 42 подалгебры в таблице 8;
 (1,9,13,4,1) – 84 подалгебра в таблице 6 и 21 подалгебра в таблице 8.

Таблица 8

№	Тип решетки	Число подалгебр в подалгебре данного типа	Количество подалгебр данного типа	Количество подалгебр данной размерности
1	(1,6,8,4,1)	20	21	497
2	(1,7,11,1,1)	21	14	
3	(1,8,12,6,1)	28	84	
4	(1,9,11,5,1)	27	42	
5	(1,9,13,4,1)	28	84	
6	(1,10,13,3,1)	28	28	
7	(1,11,17,7,1)	37	126	
8	(1,12,18,8,1)	40	84	
9	(1,12,20,9,1)	43	14	

3.6. Классификация четырехмерных подалгебр в алгебре матриц третьего порядка над полем из двух элементов

Таблица 9

Тип подалгебры	Порождающие элементы	Определяющие соотношения						Количество подалгебр	Тип решетки подалгебр
1	r_1, r_2, e (13, 5, 274)		r_1	r_2	e			21	(1,6,8,4,1)
		r_1	r_1^2	r_1^2	r_1				
		r_2	0	0	r_2				
		e	r_1	r_2	e				
2	r_1, r_2, e		r_1	r_2	e			21	(1,9,13,4,1)
		r_1	r_1^2	r_1^2	r_1+r_2				
		r_2	0	0	0				
		e	r_1	r_2	e				

3	r_1, r_2, e			r_1	r_2	e		21	(1,9,13,4,1)
			r_1	r_1^2	r_1^2	0			
			r_2	0	0	0			
			e	r_2	r_2	e			
4	r_1, r_2, e			r_1	r_2	e		21	(1,9,13,4,1)
			r_1	r_1^2	r_1^2	r_1			
			r_2	0	0	r_2			
			e	r_2	r_2	e			
5	r_1, r_2, e			r_1	r_2	e		21	(1,9,13,4,1)
			r_1	r_1^2	r_1^2	0			
			r_2	0	0	0			
			e	r_1+r_2	0	e			
6	r_1, r_2, e			r_1	r_2	e		21	(1,9,11,5,1)
			r_1	r_1^2	r_1^2	r_1+r_2			
			r_2	0	0	0			
			e	r_2	r_2	e			
7	r_1, r_2, e			r_1	r_2	e		21	(1,9,11,5,1)
			r_1	r_1^2	r_1^2	r_2			
			r_2	0	0	r_2			
			e	r_1+r_2	0	e			
8	r_1, r_2, a, a^2			r_1	r_2	a	a^2	7	(1,7,11,1,1)
		r_1	0	0	0	0	0		
		r_2	0	0	0	0	0		
		a	r_2	r_1+r_2	a^2	$a+a^2$			
		a^2	r_1+r_2	r_1	$a+a^2$	a			
9	r_1, r_2, a, a^2			r_1	r_2	a	a^2	7	(1,7,11,1,1)
		r_1	0	0	r_2	r_1+r_2			
		r_2	0	0	r_1+r_2	r_1			
		a	0	0	a^2	$a+a^2$			
		a^2	0	0	$a+a^2$	a			
10	e, r, a, a^2			e	r	a	a^2	42	(1,8,12,6,1)
			e	e	r	0	0		
			r	0	0	r	r		
			a	0	0	a^2	a		
			a^2	0	0	a	a^2		
11	e, r, a, a^2			e	r	a	a^2	42	(1,8,12,6,1)
			e	e	0	0	0		
			r	r	0	0	0		
			a	r	0	a^2	a		
			a^2	r	0	a	a^2		
12	e_1, e_2, r_1, r_2			e_1	e_2	r_1	r_2	28	(1,10,13,3,1)
			e_1	e_1	0	r_1	0		

			e_2	0	e_2	0	r_2			
			r_1	0	r_1	0	e_1			
			r_2	r_2	0	e_2	0			
13	e_1, e_2, r_1, r_2			e_1	e_2	r_1	r_2		14	(1,11,17,7,1)
			e_1	e_1	0	r_1	r_2			
			e_2	0	e_2	0	0			
			r_1	0	r_1	0	0			
			r_2	0	0	0	0			
14	e_1, e_2, r_1, r_2			e_1	e_2	r_1	r_2		14	(1,11,17,7,1)
			e_1	e_1	0	0	0			
			e_2	0	e_2	r_1	0			
			r_1	r_1	0	0	0			
			r_2	r_2	0	0	0			
15	e_1, e_2, r_1, r_2			e_1	e_2	r_1	r_2		10	(1,12,20,9,1)
			e_1	e_1	0	r_1	r_2			
			e_2	0	e_2	0	0			
			r_1	0	r_1	0	0			
			r_2	0	r_2	0	0			
		ИТОГО:							311	8

Библиографический список

1. Биркгоф Г., Барти Т. К. Современная прикладная алгебра; пер. с англ. Ю. И. Манина. – Изд. 2-е, стер. – М.: Лань, 2005. – 400 с.
2. Биркгоф, Г. Теория решеток; пер. с англ. В. Н. Салий под ред. Л. А. Скорнякова. – М.: Наука, 1984. – 568 с.
3. Гантмахер Ф.Р. Теория матриц. – 4 изд. – М.: Наука. Гл. ред. физ.-мат. лит. 1988.
4. Гретцер, Г. Общая теория решеток; пер. с англ. А. Д. Больбота, В. А. Горбунова, В. И. Туманова под ред. Д. М. Смирнова. – М. : Мир, 1982. – 456 с.
5. Калужнин, Л. А. Введение в общую алгебру. – М.: Наука, 1973. – 448 с.
6. Коробков С. С. Введение в теорию решеток: Учеб. пособие по спец. курсу. Урал. гос. пед. ун-т. — Екатеринбург: Б.и., 1996. – 64с.
7. Курош А. Г. Курс высшей алгебры: Учеб. для студентов вузов по спец. "Математика", "Приклад. математика". – 13-е изд., стер. – СПб.: Лань, 2004. – 432с.
8. Курош А. Г. Лекции по общей алгебре: учебник. – СПб.: Лань, 2005. – 560 с.
9. Коробков С.С. Вычисления в матричных алгебрах (Прикладные аспекты алгебры и информатики). (Рукопись). Екатеринбург, 2014.
10. GAPManual. Режим доступа: <http://www.gap-system.org/Doc/manuals.html>.
11. Гришина А.А. Подалгебры матричной алгебры $M_3(GF(2))$. Дипломная работа. УрГПУ. Екатеринбург. 2003.
12. Barnes D.W. Lattice isomorphisms of associative algebras //J. Austral. Math. Soc. 1966. V. 6. № 1. P. 106 – 121.
13. Система компьютерной алгебры GAP – Exponenta. Режим доступа: www.exponenta.ru/soft/others/gap/1.asp
14. GAP Manual. Режим доступа: <http://www.gap-system.org/Doc/manuals.html>
15. Graph Online URL: <http://graphonline.ru/>

Приложения

Приложение 1

Программа №1	
Текст программы	Комментарии
Sub:=[];	Создание массива
RRE:=[];	Создание массива
b:=0;	Обнуление элемента b
RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR
ID:=[2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка над полем GF(2)
El:=Elements(A);	Создание массива элементов алгебры A
for i in RR do	Начало цикла
for k in ID do	Начало цикла
B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	Записывает подалгебру алгебры A, порожденную элементами: El[i[1]],El[i[2]],El[k]

if Size(B)=16 then	Проверка условия
if El[k]*El[i[1]]=El[i[1]] and El[i[1]]*El[k]=El[i[1]] and El[k]*El[i[2]]=El[i[2]] and El[i[2]]*El[k]=El[i[2]] then	Таблица умножения из Пирсовского разложения
sub:=Elements(B);	Нахождение всех матриц
AddSet(Sub,sub);	Запись в массив Sub
if Size(Sub) > b then	Проверяем размер массива Sub
Add(RRE,[i[1],i[2],k]);	Добавляем в массив RRE элементы i[1],i[2],k
b:=Size(Sub);	Находим число всех матриц
fi;fi;fi;	Закрытие всех циклов
od; od;	Конец цикла в цикле; конец цикла
Sort(RRE);	Сортировка массива RRE
PrintTo("4ER1=R1_R1E=R1_R2E=R2=ER2.dan","RRE: = ",RRE, ";","\\n"," RRE =",Size(RRE),"\\n","Sub1:=",Sub,";","\\n");	Вывод на экран

Приложение 2

Программа №4		
№	Текст программы	Комментарии
1	Sub:=[];	Создание массива

2	RRE:=[];	Создание массива
3	b:=0;	Обнуление элемента b
4	RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR
5	ID:=[2, 4, 6, 8, 1, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 21, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
6	A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка над полем GF(2)
7	El:=Elements(A);	Создание массива элементов алгебры A
8	for i in RR do	Начало цикла
9	for k in ID do	Начало цикла
1	B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	Записывает подалгебру алгебры A, порожденную элементами: El[i[1]],El[i[2]],El[k]
11	if Size(B)=16 then	Проверка условия
12	if El[k]*El[i[1]]=El[i[1]] and El[i[1]]*El[k]=El[i[1]]+El[i[2]] and El[k]*El[i[2]]=El[i[2]] and El[i[2]]*El[k]=El[1] then	Таблица умножения из Пирсовского разложения
16	sub:=Elements(B);	Нахождение всех матриц
	AddSet(Sub,sub);	Запись в массив Sub
	if Size(Sub) > b then	Проверяем размер массива Sub

	Add(RRE,[i[1],i[2],k]);	Добавляем в массив RRE элементы i[1],i[2],k
	b:=Size(Sub);	Находим число всех матриц
	fi;fi;fi;	Закрытие всех циклов
	od; od;	Конец цикла в цикле; конец цикла
	Sort(RRE);	Сортировка массива RRE
	PrintTo("4ER1=R1_R1E=R1+R2_R2E=0_ER2=R2.dan", "RRE:=", RRE, ":", "\n", " RRE =", Size(RRE), "\n", "Sub2:=", Sub, ":", "\n");	Вывод на экран

Приложение 3

Программа №5		
№	Текст программы	Комментарии
1.	Sub:=[];	Создание массива
2.	RRE:=[];	Создание массива
3.	b:=0;	Обнуление элемента b
4.	RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR
5.	ID:=[2, 4, 6, 8, 1, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 21, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
6.	A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка

		над полем GF(2)
7.	El:=Elements(A);	Создание массива элементов алгебры A
8.	for i in RR do	Начало цикла
9.	for k in ID do	Начало цикла
10.	B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	Записывает подалгебру алгебры A, порожденную элементами: El[i[1]],El[i[2]],El[k]
11.	if Size(B)=16 then	Проверка условия
12.	if El[k]*El[i[1]]=El[i[1]]+El[i[2]] and El[i[1]]*El[k]=El[i[2]] and El[k]*El[i[2]]=El[1] and El[i[2]]*El[k]=El[i[2]] then	Таблица умножения из Пирсовского разложения
13.	sub:=Elements(B);	Нахождение всех матриц
14.	AddSet(Sub,sub);	Запись в массив Sub
15.	if Size(Sub) > b then	Проверяем размер массива Sub
16.	Add(RRE,[i[1],i[2],k]);	Добавляем в массив RRE элементы i[1],i[2],k
17.	b:=Size(Sub);	Находим число всех матриц
18.	fi;fi;fi;	Закрытие всех циклов
19.	od; od;	Конец цикла в цикле; конец цикла
20.	Sort(RRE);	Сортировка массива RRE
21.	PrintTo("4ER1=R1+R2_R1E=R2_R2E=R2_ER2=0.dan", "RRE:=",RRE,";", "\n", " RRE =",Size(RRE),"\n", "Sub3:=", Sub,";", "\n");	Вывод на экран

Результат работы программы выглядит следующим образом:

RRE:= [[13, 5, 273], [32, 5, 275], [35, 33, 258], [67, 3, 273],
 [79, 7, 273], [92, 28, 281], [97, 65, 18], [120, 64, 281],
 [133, 129, 18], [137, 9, 258], [171, 41, 258], [190, 64, 260],
 [222, 7, 275], [229, 193, 18], [244, 41, 266], [328, 3, 277],
 [334, 326, 337], [375, 28, 317], [435, 433, 386], [441, 9, 290],
 [477, 456, 467]];
 |RRE|=21

Приложение 4

Программа №6	
Текст программы	Комментарии
Sub:=[];	Создание массива
RRE:=[];	Создание массива
b:=0;	Обнуление элемента b
RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR
ID:=[2, 4, 6, 8, 1, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 21, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка над полем GF(2)
El:=Elements(A);	Создание массива элементов алгебры A
for i in RR do	Начало цикла
for k in ID do	Начало цикла
B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	Записывает подалгебру алгебры A, порожденную элементами: El[i[1]],El[i[2]],El[

	k]
if Size(B)=16 then	Проверка условия
if El[k]*El[i[1]]=El[i[2]] and El[i[1]]*El[k]=El[i[1]] and El[k]*El[i[2]]=El[i[2]] and El[i[2]]*El[k]=El[i[2]] then	Таблица умножения из Пирсовского разложения
sub:=Elements(B);	Нахождение всех матриц
AddSet(Sub,sub);	Запись в массив Sub
if Size(Sub) > b then	Проверяем размер массива Sub
Add(RRE,[i[1],i[2],k]);	Добавляем в массив RRE элементы i[1],i[2],k
b:=Size(Sub);	Находим число всех матриц
fi;fi;fi;	Заккрытие всех циклов
od; od;	Конец цикла в цикле; конец цикла
Sort(RRE);	Сортировка массива RRE
PrintTo("4ER1=R2_R1E=R1_R2E=ER2=R2.dan","RRE:=", ",RRE,",";","\\n"," RRE =",Size(RRE),"\\n","Sub4:=",Sub,",";","\\n");	Вывод на экран

Результат работы программы выглядит следующим образом:

```

RRE:= [ [ 13, 5, 258 ], [ 32, 5, 260 ], [ 35, 33, 273 ], [ 67, 3, 18 ],
[ 79, 7, 50 ], [ 92, 28, 18 ], [ 97, 65, 258 ], [ 120, 64, 50 ],
[ 133, 129, 273 ], [ 137, 9, 18 ], [ 171, 41, 22 ], [ 190, 64, 22 ],
[ 222, 7, 54 ], [ 229, 193, 260 ], [ 244, 41, 54 ], [ 328, 3, 22 ],
[ 334, 326, 258 ], [ 375, 28, 54 ], [ 435, 433, 273 ], [ 441, 9, 50 ],
[ 477, 456, 260 ] ];
|RRE|=21

```

Приложение 5

Программа №7	
Текст программы	Комментарии
Sub:=[];	Создание массива
RRE:=[];	Создание массива
b:=0;	Обнуление элемента b
RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR
ID:=[2, 4, 6, 8, 1, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 21, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка над полем GF(2)
El:=Elements(A);	Создание массива элементов алгебры A
for i in RR do	Начало цикла
for k in ID do	Начало цикла
B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	Записывает подалгебру A, порожденную элементами: El[i[1]],El[i[2]],El[k]
if Size(B)=16 then	Проверка условия
if El[k]*El[i[1]]=El[i[2]] and El[i[1]]*El[k]=El[i[1]] and El[k]*El[i[2]]=El[i[2]] and El[i[2]]*El[k]=El[i[2]] then	Таблица умножения из Пирсовского разложения
sub:=Elements(B);	Нахождение всех матриц

AddSet(Sub,sub);	Запись в массив Sub
if Size(Sub) > b then	Проверяем размер массива Sub
Add(RRE,[i[1],i[2],k]);	Добавляем в массив RRE элементы i[1],i[2],k
b:=Size(Sub);	Находим число всех матриц
fi;fi;fi;	Закрытие всех циклов
od; od;	Конец цикла в цикле; конец цикла
Sort(RRE);	Сортировка массива RRE
PrintTo("4R1E=0_ER1=R1+R2_R2E=ER2=0.dan","RRE:=",RRE,";", "\n", " RRE =",Size(RRE), "\n", "Sub5:=",Sub,";", "\n");	Вывод на экран

Результат работы программы выглядит следующим образом:

```
RRE:= [ [ 13, 5, 17 ], [ 32, 5, 19 ], [ 35, 33, 2 ], [ 67, 3, 257 ],
[ 79, 7, 145 ], [ 92, 28, 257 ], [ 97, 65, 17 ], [ 120, 64, 217 ],
[ 133, 129, 2 ], [ 137, 9, 257 ], [ 171, 41, 66 ], [ 190, 64, 196 ],
[ 222, 7, 147 ], [ 229, 193, 10 ], [ 244, 41, 74 ], [ 328, 3, 261 ],
[ 334, 326, 17 ], [ 375, 28, 293 ], [ 435, 433, 2 ], [ 441, 9, 289 ],
[ 477, 456, 19 ] ];
|RRE|=21
```

Приложение 6

Программа №8	
Текст программы	Комментарии
Sub:=[];	Создание массива
RRE:=[];	Создание массива
b:=0;	Обнуление элемента b
RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR

ID:=[2, 4, 6, 8, 1, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 21, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка над полем GF(2)
El:=Elements(A);	Создание массива элементов алгебры A
for i in RR do	Начало цикла
for k in ID do	Начало цикла
B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	Записывает подалгебру алгебры A, порожденную элементами: El[i[1]],El[i[2]],El[k]
if Size(B)=16 then	Проверка условия
if El[k]*El[i[1]]=El[i[2]] and El[i[1]]*El[k]=El[i[1]]+El[i[2]] and El[k]*El[i[2]]=El[i[2]] and El[i[2]]*El[k]=El[1] then	Таблица умножения из Пирсовского разложения
sub:=Elements(B);	Нахождение всех матриц
AddSet(Sub,sub);	Запись в массив Sub
if Size(Sub) > b then	Проверяем размер массива Sub
Add(RRE,[i[1],i[2],k]);	Добавляем в массив RRE элементы i[1],i[2],k
b:=Size(Sub);	Находим число всех матриц
fi;fi;fi;	Закрытие всех циклов
od; od;	Конец цикла в цикле; конец цикла

Sort(RRE);	Сортировка массива RRE
PrintTo("4R1E=R1+R2_ER1=R2_R2E=0_ER2=R2.dan", "RRE:=",RRE,";", "\n", " RRE =",Size(RRE), "\n", "Sub6:=",Sub,";", "\n");	Вывод на экран

```
RRE:= [ [ 13, 5, 2 ], [ 32, 5, 4 ], [ 35, 33, 17 ], [ 67, 3, 2 ],
[ 79, 7, 2 ], [ 92, 28, 10 ], [ 97, 65, 257 ], [ 120, 64, 10 ],
[ 133, 129, 257 ], [ 137, 9, 17 ], [ 171, 41, 17 ], [ 190, 64, 19 ],
[ 222, 7, 4 ], [ 229, 193, 257 ], [ 244, 41, 25 ], [ 328, 3, 6 ],
[ 334, 326, 66 ], [ 375, 28, 46 ], [ 435, 433, 145 ], [ 441, 9, 49 ],
[ 477, 456, 196 ] ];
|RRE|=21
```

Приложение 7

Программа №9	
Текст программы	Комментарии
Sub:=[];	Создание массива
RRE:=[];	Создание массива
b:=0;	Обнуление элемента b
RR:= [[13, 5], [32, 5], [35, 33], [67, 3], [79, 7], [92, 28], [97, 65], [120, 64], [133, 129], [137, 9], [171, 41], [190, 64], [222, 7], [229, 193], [244, 41], [328, 3], [334, 326], [375, 28], [435, 433], [441, 9], [477, 456]];	Массив RR
ID:=[2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив ID
A:=MatAlgebra(GF(2),3);	Построение алгебры матриц третьего порядка над полем GF(2)
El:=Elements(A);	Создание массива элементов алгебры A
for i in RR do	Начало цикла
for k in ID do	Начало цикла
B:=Subalgebra(A,[El[i[1]],El[i[2]],El[k]]);	Записывает подалгебру алгебры A, порожденную элементами: El[i[1]],El[i[2]],El[k]

if Size(B)=16 then	Проверка условия
if El[k]*El[i[1]]=El[1] and El[i[1]]*El[k]=El[i[2]] and El[k]*El[i[2]]=El[1] and El[i[2]]*El[k]=El[i[2]] then	Таблица умножения из Пирсовского разложения
sub:=Elements(B);	Нахождение всех матриц
AddSet(Sub,sub);	Запись в массив Sub
if Size(Sub) > b then	Проверяем размер массива Sub
Add(RRE,[i[1],i[2],k]);	Добавляем в массив RRE элементы i[1],i[2],k
b:=Size(Sub);	Находим число всех матриц
fi;fi;fi;	Закрытие всех циклов
od; od;	Конец цикла в цикле; конец цикла
Sort(RRE);	Сортировка массива RRE
PrintTo("4RRE=0_ERR=R2.dan","RRE:=",RRE,";"", "\n", " RRE =",Size(RRE),"\n","Sub7:=",Sub,";"", "\n");	Вывод на экран

RRE:= [[13, 5, 257], [32, 5, 257], [35, 33, 257], [67, 3, 17],
[79, 7, 49], [92, 28, 25], [97, 65, 2], [120, 64, 57],
[133, 129, 17], [137, 9, 2], [171, 41, 6], [190, 64, 8],
[222, 7, 55], [229, 193, 4], [244, 41, 46], [328, 3, 17],
[334, 326, 321], [375, 28, 25], [435, 433, 385], [441, 9, 2],
[477, 456, 449]];
|RRE|=21

Приложение 8

Массив матриц алгебры $A = M_3(GF(2))$

[illegible]

59

60

61

62

64

65

[illegible]

67